Doc Code: AP.PRE.REQ

PTo/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
550-482	

Application Number	Filed
10/714,520	November 17, 2003
First Named Inventor: BELNET	
Art Unit: 2189	Examiner: Flournoy, Horace L.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ Applicant/Inventor

☐ Assignee of record of the entire interest. See 37 C.F.R. § 3.71. Statement under 37 C.F.R. § 3.73(b) is enclosed. (Form PTO/SB/96)

☒ Attorney or agent of record 33,149 (Reg. No.)

☐ Attorney or agent acting under 37CFR 1.34.
Registration number if acting under 37 C.F.R. § 1,34 _____

Signature

John R. Lastova
Typed or printed name

703-816-4025
Requester's telephone number

August 23, 2006
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.*

☒ *Total of 1 form/s are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Belnet et al

Atty. Ref.: 550-482; Confirmation No. 8029

Appl. No. 10/714,520

TC/A.U. 2189

Filed: November 17, 2003

Examiner: Flournoy, Horace L.

For: TECHNIQUE FOR ACCESSING MEMORY IN A DATA PROCESSING APPARATUS

* * * * * * * * * * * *

August 23, 2006

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ARGUMENTS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

Error #1: Gardner Fails To Teach The Claimed Secure And Non-Secure Domains.

In claims 1 and 10, data security is managed at the hardware level on a domain basis. Data handled by the secure domain is not accessible from the non-secure domain. A domain signal issued with each memory access request is used to determine whether the access defined by any particular memory access request is allowed to proceed. If the domain signal identifies that the memory access request pertains to a non-secure domain, then that access request is not allowed to proceed if the memory access request is seeking to access secure data.

Gardner protects user application data so that it can be kept secret from root and other users. There are four privilege levels PLO to PL3: PL0 is the most privileged level of the processor, and PL3 is the least privileged level. Paragraph 0189 and Figure 6 describe how a user application operating at the least privileged level PL3 can keep its data secure from other users. Gardner uses protection keys which allow a secure user application "to access a page of memory in memory 74 that nobody else can access, including root or anything running at PL2 or

above" (0190). The protection keys are inserted into protection key registers by code executing at the protection level PLO (0191).

The Examiner refers to paragraph 0189 as teaching secure and non-secure domains. This paragraph does not mention domains at all. Instead, paragraph 0189 merely refers to secure user applications and non-secure user applications, both of which are user applications running at the lowest privilege level PL3. Gardner does not control access to data based on domains and associated domain signals included with memory access requests. Instead, Gardner uses protection keys managed by the highest privilege level PLO to keep the data of particular "secure" user applications secret, and hence, not accessible by other applications.

Claims 1 and 10 use three different terms: modes, programs, and domains. The processor can operate in a number of different modes of operation, for example a user mode, a supervisor mode, etc. In a particular mode of operation, the processor can execute programs. For example, a user application or program will typically be executed in a non-privileged mode of operation. Example privileged modes include a system mode and a supervisor mode. In addition to modes of operation and execution of programs, the claimed processor can operate in a secure domain and a non-secure domain. As claimed, access to data stored in memory is performed on a domain basis to ensure that data pertaining to the secure domain is not accessed from the non-secure domain. The Examiner equates modes of operation to the "user processes" identified in paragraph 0189. In Gardner, all user applications run at the same PL3 privilege level (0189 and Fig. 1). But even allowing the Examiner's view of different user processes as different modes of operation, it is not clear what teaching in Gardner the Examiner is equating to the secure domain and the non-secure domain.

Paragraph 0026 of Gardner refers to a "domain" and mentions that secure platform 40 ensures that one domain cannot accidentally or intentionally access another domain's memory.

Paragraphs 0031 and 0032 describe that the operating system image can be partitioned into independent protection domains which operate at the PL2 privilege level. The multiple protection domains are protected from each other through the memory protection capabilities of the four privilege level processor hardware 32 (paragraph 0032). But these protection domains are different from the claimed secure and non-secure domains used to keep data secure. Gardner's protection domains are not the mechanism Gardner uses to keep data secure. Rather, Gardner uses protection keys as described earlier.

In short, there is no disclosure in Gardner of "a secure domain and a non-secure domain" where "in the secure domain devices of the data processing apparatus hav[e] access to secure data which is not accessible in the non-secure domain," as recited in claims 1 and 10.

Error #2: Gardner Lacks Plural Devices That Can Issue A Memory Access Request Including A Domain Signal Identifying Whether The Memory Access Request Pertains To A Secure Domain Or Non-Secure Domain.

Gardner lacks the *claimed* plural devices. The Examiner refers to paragraphs 0031 and 0034 as showing a plurality of devices. Paragraph 0031 describes independent protection domains formed by partitioning the operating system image. Multiple devices are not described. Paragraph 34 describes a system management counsel (SMC) that may be formed from separate independent processors. But it is not apparent how they can be the claimed plural devices "each operable to issue a memory access request pertaining to either said secure domain or said non-secure domain." None of the SMC processors issues memory access requests.

Gardner also does not disclose the claimed memory access request which includes a domain signal identifying whether the memory access request pertains to the secure domain or non-secure domain. The Examiner suggests that the claimed memory access request including the domain signal is disclosed by paragraph 0189. But again, paragraph 0189 makes no reference to domains at all, and merely describes that secure user applications (i.e., applications

that want their data to be kept secure from other users) are distinguishable from non-secure user applications through appropriate setting of an ELF header. An ELF header describes information about a particular piece of software code: the layout of an executable file, and contains information such as the start address of the code, the type of the code, and other information. Although this information enables different types of applications to be distinguished from one another, it has nothing to do with issuing memory access requests or managing access to data associated with those memory access requests. In contrast, claims 1 and 10 recite that the domain signal is included with each memory access request.

The Examiner refers to a secure ELF loader included among the PL0 services provided by the SPK software 36 (Figure 1 makes clear that SPK is a piece of software running at the PL0 level) for securely loading ELF headers pertaining to secure user applications in a secure manner so that information about those secure user applications is kept secure. But this has nothing to do with devices issuing memory access requests when they desire access to an item of data stored in memory. Nor is the ELF loader loading an ELF header the same as a memory access request that includes a domain signal identifying whether the memory access request pertains to a secure domain or a non-secure domain.

Error #3: Allocating Memory Is Not The Same As Accessing Memory

The Examiner equates allocating secure memory with accessing memory. This is an error. As Gardner describes in that paragraph, the SPK software's PL0 level service allocates memory pages which are protected using a protection key unique to a user's process. The claimed memory access requests are the mechanism by which a device seeks access to a data item in memory. The mechanism by which particular regions of memory are allocated is simply not relevant to controlling how secure memory is accessed to store secure data and non-secure memory to store non-secure data.

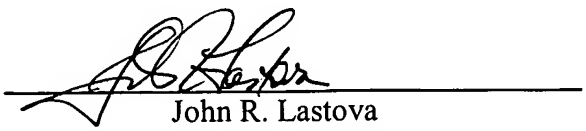
Error #4: Gardner's ELF Header Is Not Used "To Determine Whether The Access Defined By The Memory Access Request Is Allowed To Proceed"

Claims 1 and 10 recite that the domain signal is included with each memory access request. The domain signal is used "to determine whether the access defined by the memory access request is allowed to proceed" (quoted from claim 10). No such domain signal or use of that domain signal to determine whether to allow an access request to proceed is disclosed in Gardner. The Examiner reads this claim feature onto Gardner's ELF header, and after discussing paragraphs 189 and 193, the Examiner concludes that "Gardner teaches that SPK 36 can allocate memory while using the ELF to distinguish that memory allocation between secure and non-secure." This conclusion is simply not supportable. Paragraph 193 discusses allocation (not access) of memory. Paragraph 189 describes loading the ELF headers associated with secure user allocations in a secure manner, which has nothing to do with memory allocation. Accordingly, the ELF headers are not used "to determine whether the access defined by the memory access request is allowed to proceed."

Given these multiple clear errors—any one of which defeats the anticipation rejection based on Gardner, the final rejection should be withdrawn and the application passed to allowance.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100